International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.4205

(02/2019)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Internet of things and smart cities and communities – Requirements and use cases

---

Requirements and reference model of IoT-related crowdsourced systems

Recommendation ITU-T Y.4205

ITU-T

International Telecommunication Union

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	Y.3500–Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	**Y.4100–Y.4249**
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899
Evaluation and assessment	Y.4900–Y.4999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.4205

Requirements and reference model of IoT-related crowdsourced systems

Summary

Recommendation ITU-T Y.4205 introduces the concept of crowdsourced systems, as well as the reference model of IoT-related crowdsourced systems for the support of Internet of things (IoT) applications and services to be provided via systems employing crowdsourcing principles. It addresses IoT-related crowdsourced systems in terms of functional requirements and the reference model as well as identifying relevant security, privacy and trust issues.

In particular, the main contributions of Recommendation ITU-T Y.4205 can be summarized as follows:

– It identifies and provides the motivation for IoT-related crowdsourced systems (recent technological advancements and relevant emerging trends).

– It provides definitions of terms that are central when discussing crowdsourcing and crowdsourced systems, thus providing a basis of common understanding. So far, such terms have been used in layman's terms, outside a formal standardised framework; a practice which has led to ambiguity hindering further development of such systems. It is worth noting that the said definitions have been elicited via a rigorous methodology from a plethora of publications (both by academia and the industry); more information can be found in the body of the Recommendation.

– It provides a high-level reference model identifying the key layers and components of crowdsourced systems. The model does not dictate nor indicates a specific implementation or approach for building IoT-related crowdsourced systems. On the contrary, it provides a nominal model that facilitates the design and development of such systems by providing a common basis of reference.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.4205	2019-02-13	20	11.1002/1000/13859

Keywords

Crowdsensing, crowdsourcing, crowdsourced resource, crowdsourced systems, Internet of things.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Introduction

Recent technological advancements and corresponding trends have driven the rise of new networking and computing paradigms. For instance, high acceptance rates of smartphones, smart watches and other smart gadgets have led to an abundance of devices with significant communication and sensing capabilities. In addition, the increasing popularity of single-board computers (SBCs) enables the use of highly affordable platforms in the context of "made at home" projects.

This abundance of resources has led to new networking and computing paradigms, which enable crowd-provided resources to operate in a collaborative manner in order to carry out tasks or provide services. The embedded networking and sensing capabilities of such resources (e.g., smartphones) as well as their ad-hoc nature makes them highly relevant to Internet of things (IoT) systems. For instance, a ubiquitous sensor network (USN) can augment its resources and capabilities in a scalable and financially viable way by opportunistically incorporating crowdsourced resources. Such crowdsourcing methods in the context of IoT support novel economic and business models that are based on collaborative schemes, bottom up innovation and citizen-oriented data.

In order for the true potential of crowdsourced systems to unfold, several challenges need to be addressed. As a new and emerging paradigm, the notion of a crowdsourced system needs to be clearly defined in order for its particular characteristics and the derived challenges to be identified. The added value of a crowdsourced system relies on the size of the participating crowd and the corresponding number of resources. However, the great variety of software and hardware platforms and the lack of common development libraries, middleware and virtualization techniques hinder the development of truly interoperable applications and services. Also, the highly personal nature of crowdsourced resources drives the need for particular security, trust and privacy considerations.

Recommendation ITU-T Y.4205

Requirements and reference model of IoT-related crowdsourced systems

1 Scope

This Recommendation provides definitions for crowdsourced and crowdsensing systems. It also outlines the requirements and general characteristics of IoT-related crowdsourced systems for the support of IoT applications and services. It identifies the risks and challenges that a crowdsourced system should take into consideration, its reference model as well as considerations regarding security, privacy and trust.

In particular, this Recommendation covers:

– the concept of the IoT-related crowdsourced system and corresponding definitions;

– the requirements for the IoT-related crowdsourced system;

– the reference model of the IoT-related crowdsourced system;

– considerations regarding security, privacy and trust of the IoT-related crowdsourced system;

– use cases related to IoT-related crowdsourced systems;

In this Recommendation crowdsourcing in IoT-related crowdsourced systems refers not to harvesting information or knowledge from the public but to hardware or services.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Y.2012] Recommendation ITU-T Y.2012 (2010), *Functional requirements and architecture of next generation networks.*

[ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1.*

[ITU-T Y.2702] Recommendation ITU-T Y.2702 (2008), *Authentication and authorization requirements for NGN release 1.*

[ITU-T Y.2704] Recommendation ITU-T Y.2704 (2010), *Security mechanisms and procedures for NGN.*

[ITU-T Y.2720] Recommendation ITU-T Y.2720 (2009), *NGN identity management framework.*

[ITU-T Y.3041] Recommendation ITU-T Y.3041 (2013), *Smart ubiquitous networks – Overview.*

[ITU-T Y.4000] Recommendation ITU-T Y.4000/Y.2060 (2016), *Overview of the Internet of things*.

[ITU-T Y.4100] Recommendation ITU-T Y.4100/Y.2066 (2014), *Common requirements of the Internet of things.*

[ITU-T Y.4101]	Recommendation ITU-T Y.4101/Y.2067 (2017), *Common requirements and capabilities of a gateway for Internet of things applications*.
[ITU-T Y.4105]	Recommendation ITU-T Y.4105/Y.2221 (2010), *Requirements for support of ubiquitous sensor network (USN) applications and services in the NGN environment*.
[ITU-T Y.4113]	Recommendation ITU-T Y.4113 (2016), *Requirements of the network for the Internet of things.*
[ITU-T Y.4402]	Recommendation ITU-T Y.4402/F.747.4 (2013), *Requirements and functional architecture for the open ubiquitous sensor network service platform.*
[ITU-T Y.4702]	Recommendation ITU-T Y.4702 (2016), *Common requirements and capabilities of device management in the Internet of things*.
[ITU-T X.1252]	Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and definitions.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 device [ITU-T Y.4000]: With regard to the Internet of things, this is a piece of equipment with the mandatory capabilities of communication and the optional capabilities of sensing, actuation, data capture, data storage and data processing.

3.1.2 Internet of things (IoT) [ITU-T Y.4000]: A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

NOTE 1 – Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.

NOTE 2 – From a broader perspective, the IoT can be perceived as a vision with technological and societal implications.

3.1.3 privacy [ITU-T X.1252]: The right of individuals to control or influence what personal information related to them may be collected, managed, retained, accessed, and used or distributed.

3.1.4 sensor [ITU-T Y.4105]: An electronic device that senses a physical condition or chemical compound and delivers an electronic signal proportional to the observed characteristic.

3.1.5 sensor node [ITU-T Y.4105]: A device consisting of sensor(s) and optional actuator(s) with capabilities of sensed data processing and networking.

3.1.6 sensor network [ITU-T Y.4105]: A network comprised of interconnected sensor nodes exchanging sensed data by wired or wireless communication.

3.1.7 ubiquitous sensor network (USN) [ITU-T Y.4105]: A conceptual network built over existing physical networks which makes use of sensed data and provides knowledge services to anyone, anywhere and at any time, and where the information is generated by using context awareness.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 crowd: The term is used to collectively refer to the contributors (crowdsourcees) of a crowdsourced system, as well as to the resources that are provided to a crowdsourced system.

3.2.2 crowdsourcing participant: The person contributing to a crowdsourced system by providing and potentially benefitting from ideas, content, or access to services, hardware or other system resources. In the general case, the participant is a member of a large, open and potentially undefined group of people.

3.2.3 crowdsourced resource: The device, hardware module, service or other system resource that a crowdsourced system has been given access to by crowdsourcing participants.

3.2.4 crowdsourcer: The initiator of a crowdsourcing task. It can refer to a single person, a group of people, a corporation, an organization, etc.

3.2.5 crowdsourcing: The practice of obtaining needed services, ideas, content or other system resources by soliciting contributions from a large, open and potentially undefined group of people, rather than from employees, suppliers or identified experts through an online open call by providing incentives (financial, social, or entertainment) to all or a subset of those crowd members who participate in the crowdsourcing activity.

3.2.6 crowdsensing: The practice of employing crowdsourcing in collecting sensory data.

3.2.7 crowdsourced systems: **S**ystems that employ crowdsourcing in order to augment their constituent infrastructure and the set of provided services or collected information.

3.2.8 crowdsensing systems: A special case of crowdsourced systems in the application area of collecting sensing data via crowdsourced resources.

3.2.9 extrinsic incentive mechanism: A mechanism offering a reward in an explicit, "external" form; e.g., money or services.

3.2.10 intrinsic incentive mechanism: A mechanism offering a reward originating from within as a result of contributing or participating in an activity; e.g., experiencing self-fulfilment, joy or contributing to a greater cause.

3.2.11 opportunistic application: Regarding crowdsourced systems, in these types of applications data are collected from the crowdsourced devices automatically, without the intervention of the device owner.

3.2.12 participatory application: Regarding crowdsourced systems, in these types of applications data are collected as an explicit contribution of the crowdsourcees.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API Application Programming Interface

ICT Information and Communication Technology

IoT Internet of Things

NGN Next Generation Network

SBC Single-Board Computer

USN Ubiquitous Sensor Network

5 Conventions

The keywords "**is required**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "**is recommended**" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

The keywords "**can optionally**" and "**may**" indicate an optional requirement which is permissible, without implying any sense of being recommended. These terms are not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 IoT-related crowdsourced systems definition, description and use-cases

6.1 Working methods

As defined in clause 3.2.7, a crowdsourced system is a system that employs crowdsourcing in order to augment its constituent infrastructure and the set of provided services or collected information. The definition of crowdsourcing is based on a systematic literature review of relevant papers published in the proceedings of international, peer-reviewed conferences and journals. In particular, 652 papers were analysed by employing rigorous, scientifically replicable methods, see [b-CompScience]. From this corpus, 113 papers that provided definitions were extracted; 72 of the extracted papers were purely academic (i.e., all authors were academics) while 41 were authored or co-authored by people working in the industry. Furthermore, the background of the extracted papers spanned across several disciplines covering among others computer science, business/management and law.

6.2 Description

In the context of IoT, the two main technological enablers that can provide crowdsourced infrastructure for IoT-related crowdsourced systems are smartphones (and other smart gadgets) and single-board computers; in the future, other enablers may rise as well, such as smart wearables. A crowdsourced system can employ such devices via crowdsourcing and orchestrate their operation in the context of carrying out a task. In return, the system provides the owners of the devices with some kind of incentive, which may come in several forms referring to extrinsic (e.g., monetary or service based) incentives and/or intrinsic incentives (e.g., social ones and entertainment).

The nature of the task to be carried out can involve the computational, communicational or sensorial capabilities of the crowdsourced devices. In the particular case where the embedded sensory capabilities of the devices are used in order to collect sensing data (e.g., ambient luminance, position, sound, etc.) the system is called a crowdsensing system.

In principle, the applications of crowdsourced systems can be of two types, as first identified in [b-IEEEComm], [b-IEEEComm11]. The first type refers to participatory applications (see clause 3.2.12) in which the members of the engaged crowd need to actively contribute to the task. For instance, in a participatory sensing task individuals may be asked to record a sound sample of their current environment. The second type refers to opportunistic applications (see clause 3.2.11) in which the members of the engaged crowd grant the crowdsourced system with access to their devices in the context of the task to be performed; i.e., the granted access is not universal and unconditional but directly refers to the task to be undertaken in terms of time, space, resources to be accessed, etc. Once access has been granted, the system is free to utilize the corresponding resources without the active engagement of individuals.

A crowdsourced system can operate in a stand-alone way or it can be interconnected with other IoT systems, such as USNs, in the context of broader systems; e.g., a smart building. It may also be interfaced with services such as cloud storage and big data analytics in order for the collected data to be processed. Therefore, a crowdsourced system should follow a reference model that would enable it to be interfaced with other systems. A crowdsourced system should also provision in its design the human factor and in particular aspects such as security, privacy and trust.

Crowdsourced systems provide a method for opportunistically augmenting IoT and sensing infrastructure in a scalable and financially viable way. For instance, crowdsourced systems can be used to complement and extend the already available infrastructure for smart buildings, smart cities and communities. Also, the high acceptance rate of the corresponding enabling technologies by the general public (e.g., smartphones) alleviates the problem of IoT infrastructure deployment in an area of interest. Finally, crowdsourced systems can leverage the collective intelligence of people in the context of participatory applications.

6.3 Use cases

To exemplify the concepts behind crowdsourced systems, the following indicative use-cases are given.

6.3.1 Adaptive in-door luminance for a smart airport

In a smart airport equipped with IoT-enabled light control, travellers provide luminance measurements via the embedded sensors of their devices in exchange for free internet access. Measurements are then aggregated in the back end of the system into a live luminance map that is used to optimize the operation of the indoor light units of the airport.

6.3.2 Local distributed computer

Members of a local community have access to a local distributed computer that is crowdsourced. This is a distributed information and communication technology (ICT) infrastructure consisting of single-board computers provided by the members of the community. Members owning a SBC contribute to the system by installing an open-source add-on. This enables each SBC to operate as a computing cell of the distributed local computer and therefore collaboratively carry out computationally heavy tasks, such as video rendering or simulations. Access to this crowdsourced system is restricted to contributing members; thus non participants are incentivized to also contribute.

6.3.3 Optimization of public transportation for a smart city

The IoT infrastructure of a smart city is used to monitor traffic flow and quickly identify traffic jams. This enables the city to adjust traffic signals and mitigate anticipated traffic jams. City commuters provide additional information regarding their location which helps infer their current distribution and direction of commuting (e.g., that a grand portion of them is travelling towards downtown or a stadium). The aggregated information is used in scheduling dynamically adaptive bus itineraries.

7 Requirements of IoT-related crowdsourced systems

In general, IoT-related crowdsourced systems have the same functional requirements as other IoT systems. Therefore, the requirements described in [ITU-T Y.4100], [ITU-T Y.4101] and [ITU-T Y.4702] also apply to IoT-related crowdsourced systems. However, due to the unique characteristics of crowdsourced systems, these requirements need to be refined and additional ones need to be specified. Following are the requirements of IoT-related crowdsourced systems, with references to other ITU-T Recommendations where needed.

7.1 Openness

It is required that an IoT-related crowdsourced system maintains its openness as indicated by their definition in clause 3.2.7, because the driving force behind crowdsourced systems is the contributions made to the system by an undefined, open group of crowdsourcees. Such openness characterizes several aspects of IoT-related crowdsourced systems, including access to the system (see clause 7.1.1), design principles (see clause 7.1.2), and data models (see clause 7.1.3). This also relates to the non-functional requirements of interoperability, scalability, and adaptability as defined in [ITU-T Y.4100] as well as the open USN service platform [ITU-T Y.4402].

7.1.1 Openness in terms of crowd accessibility

It is required that a crowdsourced system provide a publicly accessible infrastructure supporting the mass participation of crowdsourcees. The infrastructure can provision tools for facilitating the engagement of the crowd such as webpages or smartphone applications. While access restrictions may apply depending on the application context of the system (e.g., access may be restricted to adults only or to the residents of a particular area or to registered users of a service), these must not restrict participation to a narrow or very specific group of people and should be inherent to the task at hand.

7.1.2 Openness in terms of hardware and software design

It is required that a crowdsourced system be developed by following design decisions that facilitate the participation of crowdsourcees. Towards this end, the use of modular architectures that provision future extensions of the system and the use of standardized technologies are recommended. In the cases where the crowdsourcees contribute to the system by developing a piece of hardware (e.g., a sensing device), it is recommended that several development platforms are supported. In the cases where the crowdsourcees contribute to the system by developing or deploying a piece of software, it is recommended that its hardware requirements are as generic as possible. For both hardware and software, the interfaces and application programming interfaces (APIs) used should address interoperability issues and where relevant, integration and federation issues. This requirement is related to the open interfaces requirement as mentioned in [ITU-T Y.4402].

7.1.3 Openness in terms of data

It is required that a crowdsourced system employ a standardized and open data model. This is because a crowdsourced system may collect data from a diverse set of devices with different calibrations (e.g., when the system monitors ambient environmental conditions). In this case a standardized data model would be required for efficient data management and processing. Similarly, if, in the context of a crowdsourced system, devices are required to exchange data (e.g., in order to perform some local data processing) an open data model will help mitigate interoperability issues.

7.2 Affordability and availability of system components

It is required that a crowdsourced system rely on system components (either hardware or software) that are both affordable and available to the general public. Affordability and availability imply that a crowdsourced system should not rely on specialized equipment. On the contrary, the general public should be able to obtain the needed equipment off-the-shelf (e.g., smartphones) or be able to develop it with off-the-shelf components (e.g., with SBC development platforms).

7.3 Anonymity of crowdsourcees

It is recommended that a crowdsourced cystem incorporate mechanisms that support the anonymity of individual crowdsourcees. This is interpreted as the system providing sufficient guarantees that an individual cannot be identified as a result of contributing to the system. The reason for this requirement is two-fold. First, it helps mitigate any issues related to trust and privacy that would potentially hinder contributions from the general public. Second, by definition and therefore by design, a crowdsourced system should not be dependent on particular individuals. While providing guarantees on anonymity, the system can still incorporate filter mechanisms for distinguishing sub-groups of crowdsourcees based on some attributes (e.g., demographics).

7.4 Aggregation mechanisms

It is required that a crowdsourced system incorporates aggregation mechanisms for processing crowdsourced data that are agnostic to the particular identity of the crowdsourcees. However, such mechanisms can take into consideration attributes such as reputation, trust-worthiness, etc. The aggregation mechanisms can be of two types: a) centralized aggregation mechanisms, where the data is processed after having been collected in a data repository or b) in-network aggregation mechanisms, where the nodes of the crowdsourced system process the data locally before being sent to the data repository of the system. Hybrid solutions can also be implemented combining the two types.

7.5 Abstraction mechanisms

It is recommended that a crowdsourced system provides abstraction mechanisms for each component of its architecture. These abstraction mechanisms help hide the underlying heterogeneity and diversity of each component. They also contribute towards clearly differentiating the role of each participant in the system; for instance, the crowdsourcer interacts with the crowd as a whole via corresponding APIs rather than with individual crowdsourcees. The use of abstraction mechanisms among the system components implies a modular architecture for the overall system. This contributes towards better system designs that complement other requirements (such as the anonymity of the crowd). This relates to the non-functional requirements (interoperability, scalability, reliability, etc.) and communication requirements (e.g., heterogeneous communication support) of the Internet of things as defined in [ITU-T Y.4100].

7.6 Incentive mechanisms

It is recommended that a crowdsourced system can optionally provide incentives to crowdsourcees in order to successfully engage them in a consistent and successful way. An incentive corresponds to the added value perceived by each crowdsourcee as a result of her contribution to the system. There are two categories of incentives: Intrinsic incentives reward the crowdsourcees via contentment, for instance when contributing to a greater cause or to the common good (e.g., when help fighting a disease). Extrinsic incentives consist in offering more direct rewards to the crowdsourcees, for instance via micro-payments or additional services.

8 Reference model of IoT-related crowdsourced systems

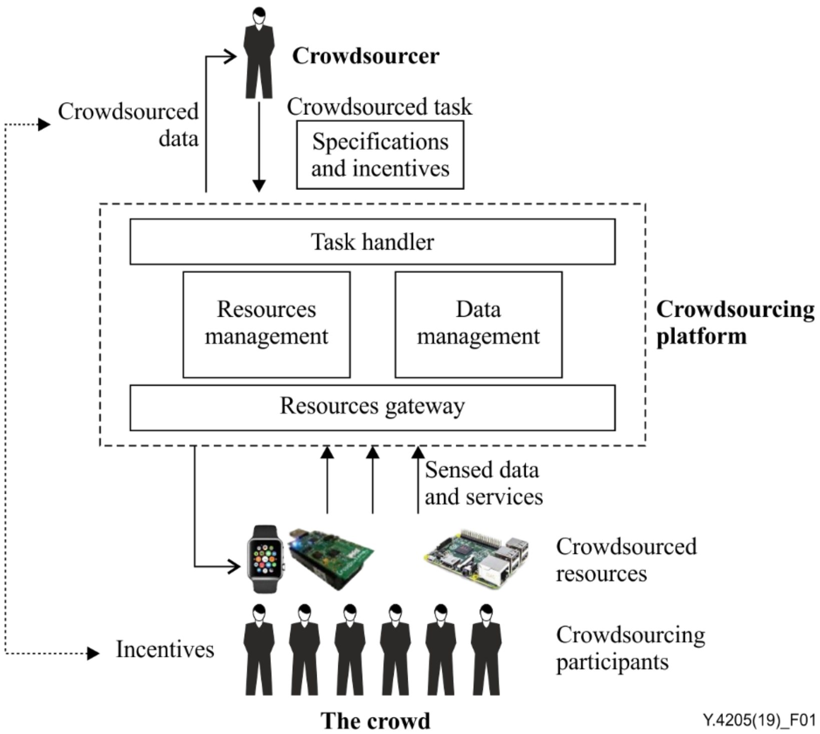

Figure 1 – The reference model for IoT-related crowdsourced systems

Figure 1 shows the reference model for IoT-related crowdsourced systems. A crowdsourced system consists of three layers arranged in a vertical manner. The top layer refers to the crowdsourcer and the task to be executed via crowdsourcing. The bottom layer refers to the crowd and the crowdsourced resources that provide the sensed data and services in the context of the task; in return incentives are received. The intermediate layer refers to the modules and services that form the core of the crowdsourcing platform; this includes the task handler at the north edge of the layer, the resource management and data management modules and the resources gateway at the south edge. This is a reference model, meaning that there is no limitation on how it can be implemented in the context of a particular crowdsourced system. Each of these elements is detailed in the following.

The crowdsourcer: The crowdsourcer describes the crowdsourced task to be executed by defining its specifications and the corresponding incentive mechanisms. The task specifications can include a description of the crowd resources to be employed (e.g., defining the type of the resource or their geographic location). The incentives provided to the crowd may be extrinsic (e.g., monetary or service based) or intrinsic (e.g., social incentives such as contributing to a greater cause).

The task handler: The task handler lies at the north edge of the crowdsourcing platform. It is the module that exposes the services of the crowdsourced system to its user(s). It enables the crowdsourcer to discover, manage and access the crowdsourced resources in a uniform manner via the corresponding modules. It also returns the results of the task to the crowdsourcer in a format that would be meaningful (e.g., results in a semantic context instead of raw values). Furthermore, it relays the task specifications and incentive mechanisms to the resource and data management modules in a proper way for the task to be compiled and executed. In general, the task handler can be regarded as an abstraction layer that hides the underlying complexity of the crowdsourced system while facilitating task composition and execution. This relates to the requirements of service composition, service management and discovery services as mentioned in [ITU-T Y.4100].

Resources management: Resources management is the module where all the information and the meta-data regarding the system resources (including the crowdsourced ones) is maintained and managed. It acts as a resource directory that supports and exposes all the necessary services for registering, discovering, and accessing resources. It also maintains meta-information that characterize each resource; e.g., its type, access method, availability, trustworthiness, etc. Typically, the resource manager should maintain information in a standardized format with the aim of (i) addressing all resources in a standardized way thus mitigating heterogeneity issues and (ii) facilitating the use of this information by other elements of the model (e.g., the crowdsourcer). This also relates to the requirements of programmable interfaces, group management, collaboration, user management, and resource usage accounting as mentioned in [ITU-T Y.4100]

Data management: Data management is the module where all collected data is stored and curated along with relevant meta-data. For example, if in the context of a crowdsensing task temperature measurements are collected, then 'data' refers to the actual temperature readings while 'meta-data' may refer to information on the time and place that these readings were measured. Typically, data and meta-data should be maintained in the data management module in a standardized format in order to address heterogeneity and interoperability issues. In this respect, Cloud and Big Data technologies can be used since a crowdsourced system is anticipated to generate big volumes of data. The data management module also provides the necessary services for storing, processing and curating data. Depending on the crowdsourced system and application, these services may be sophisticated ones; for instance, data mining mechanisms may be employed in order to extract semantically meaningful information from initial data (e.g., to generate a heat-wave alert from a set of temperature measurements). This relates to data management requirements for the IoT as mentioned in [ITU-T Y.4100] as well as for USN as mentioned in [ITU-T Y.4402].

Resources gateway: Resources gateway lies at the south edge of the crowdsourcing platform. It is the module that interconnects each individual crowdsourced resource to the crowdsourcing platform. This interconnection is performed in such a way that the underlying heterogeneity and diversity of the crowdsourced resources is hidden from the upper layers of the architectures. This enables the set of crowdsourced resources to be addressed in a uniform way thus giving rise to the crowd. This heterogeneity and diversity mitigation is achieved with the use of commonly understood interfaces via appropriate mechanisms (e.g., mobile applications for smartphones or software add-ons for SBCs). This is related to the requirements for openness of USN as mentioned in [ITU-T Y.4402].

The crowd: The crowd constitutes the foundation of a crowdsourced system. The term may refer collectively to the crowdsourced resources or to the crowdsourcees (i.e., the owners of the devices) that contribute to the system. As an example, consider the owner of a smartphone and the device per se. In the context of a crowdsourced task, the crowd provides sensed data and/or services and in return receives incentives, which may come at various forms (extrinsic or intrinsic incentives as specified earlier in this Recommendation).

9 Additional considerations of IoT-related crowdsourced systems such as privacy and security

IoT-related crowdsourced systems are able to consolidate crowdsourced resources provided by the general public. Crowdsourced resources however (typically consisted of smartphones, smart wearables and SBC computing platforms deployed at homes or work environments) pose significant issues in terms of privacy and trust due to their highly personal character. Therefore, it is required that special care is taken when designing/developing a crowdsourced system in terms of privacy and trust.

In this context, IoT-related crowdsourced systems inherit the following requirements from IoT, USN and next generation network (NGN) recommendations.

It is required that an IoT-related crowdsourced system follows the security and privacy protection requirements as mentioned in [ITU-T Y.4100].

It is required that an IoT-related crowdsourced system follows the proper management policies on authentication, authorization and access rights as mentioned in [ITU-T Y.4402].

It is required that an IoT-related crowdsourced system follows the requirements for NGN in terms of access control, authentication, non-repudiation, data confidentiality, communication security, and privacy as mentioned in [ITU-T Y.4402].

An IoT-related crowdsourced system follows the requirements on identity management security in order to protect the privacy of crowdsourcees as mentioned in [ITU-T Y.2720].

Appendix I

Indicative commercial solutions and technologies that can be used in crowdsourced systems

(This appendix does not form an integral part of this Recommendation.)

In the main body of this Recommendation several references are made to technologies and solutions in an abstract way. This is meant in order to avoid direct reference to particular commercially available solutions in order (i) not to bias the Recommendation towards particular products and (ii) in order not to restrict the presented concepts to the solutions available at the time of editing this Recommendation (the landscape of available technologies is a very dynamic one with new solutions constantly emerging).

The following list of solutions/technologies/products is meant to (i) exemplify the presented concepts and help the reader better understand the Recommendation and (ii) to provide an indicative starting point for the inexperienced reader. This list is only indicative and is not meant to restrict the means of developing crowdsourced systems in any way.

Term	**Solution/Technology/Product (indicative list)**
Smartphones	Android, iOS, Windows Mobile
Single-board computers	Arduino, Raspberry Pi, BeagleBone, Intel Galileo, Intel Edison
Distributed / Big Data storage	Apache Hadoop, MongoDB, Apache Spark, Apache Cassandra
IoT platforms	Xively, Meshify, FIWARE

Bibliography

[b-CompScience] Hosseini, M., Shahri, A., Phalp, K., Taylor, J. and Ali, R.Crowdsourcing. *A taxonomy and systematic mapping study. Computer Science Review, 17, pp.43-69, 2015*.

[b-IEEEComm] Nicholas D. Lane, Emiliano Miluzzo, Hong Lu, Daniel Peebles, Tanzeem Choudhury, Andrew T. Campbell. *A survey of mobile phone sensing. IEEE Communications Magazine, Volume: 48, Issue: 9, 2010.*

[b-IEEEComm11] Raghu K. Ganti, Fan Ye, and Hui Lei. *Mobile Crowdsensing: Current State and Future Challenges. IEEE Communications Magazine, Volume: 49, Issue: 11, 2011*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2019